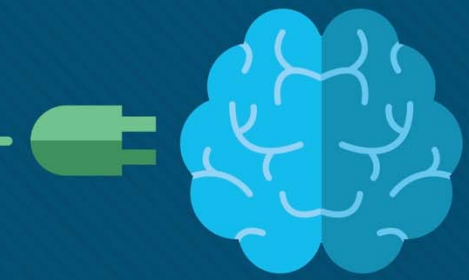
Endpoint Security dhe Analiza

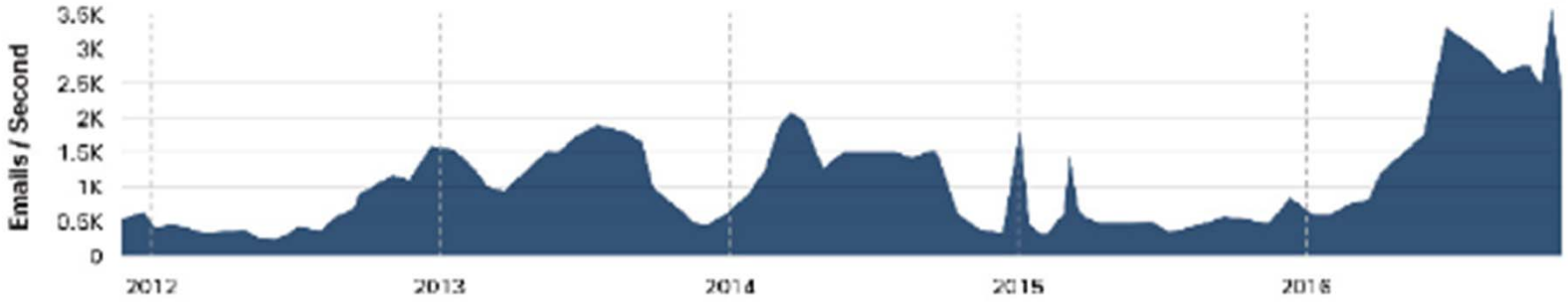


Objektivat

- Mbrojtja e Endpoint
  - Përdorni një website për analiza malware për të gjeneruar një raport analiza malware.
    - Shpjegoni metodat e zbutjes së malware.
    - Shpjegoni shënimet e regjistrit të IPS / IDS me bazë host.
    - Përdorni virustotal.com për të gjeneruar një raport analiza malware.
- Vlerësimi i Vulnerabilitetit të Endpoint
  - Klasifikoni informacionin e vlerësimit të cenueshmërisë në fund.
    - Shpjegoni vlerën e profilizimit të rrjetit dhe serverit.
    - Klasifikoni raportet e CVSS.
    - Shpjegoni kornizat e pajtueshmërisë dhe raportimin.
    - Shpjegoni se si përdoren teknika të menaxhimit të pajisjeve të sigurta për të mbrojtur të dhënat dhe pasuritë.
    - Shpjegoni se si përdoren sistemet e menaxhimit të sigurisë së informacionit për të mbrojtur asetet.

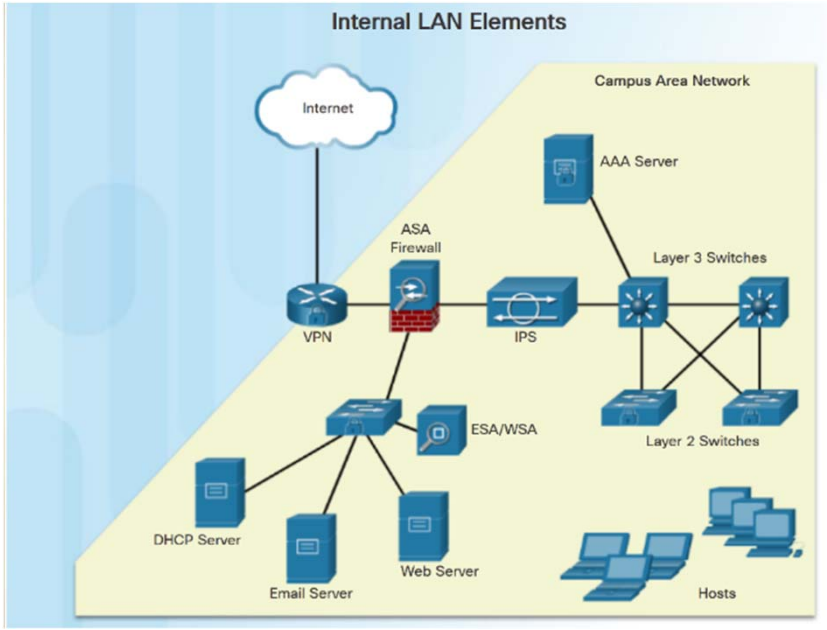
Mbrojtja Antimalware
Kërcënimet e Endpoint

- Kërcënimet e Endpoint
  - Rritja e numrit të pajisjeve për shkak të mobilitetit dhe IOT
  - Mbi 75% e organizatave përjetuan infeksione adware nga 2015-2016
  - Nga viti 2016 deri në fillim të vitit 2017, vëllimi global i spam-it u rrit në mënyrë dramatike
  - Malware që synon sistemin operativ Android Android ishte në dhjetë llojet më të zakonshme të gjetur në 2016
  - Disa lloje të zakonshme të malware mund të ndryshojnë ndjeshëm karakteristikat në më pak se 24 orë në mënyrë që të shmangin zbulimin.



Mbrojtja Antimalware
Endpoint Security

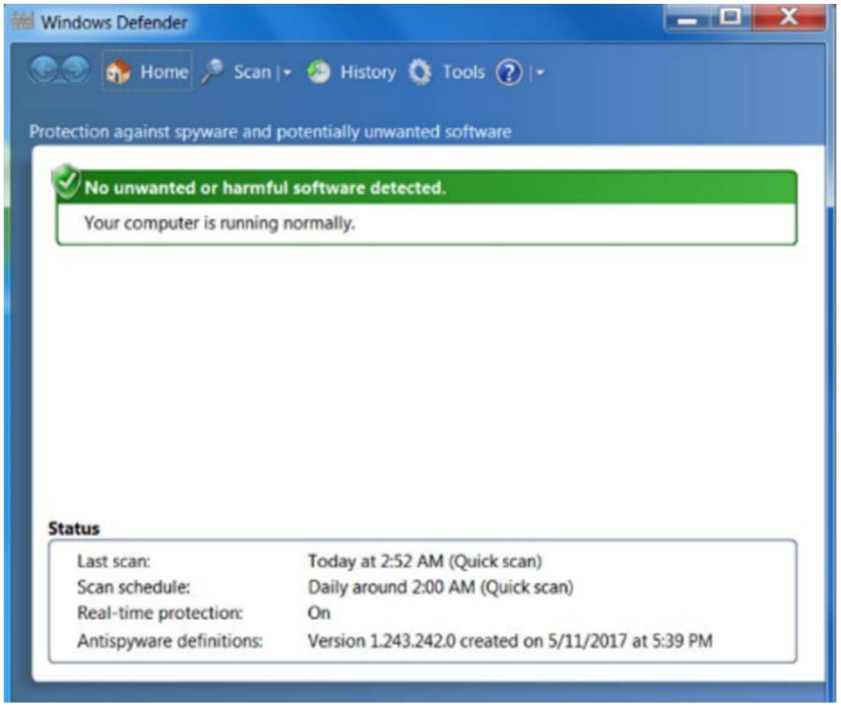
- Dy elementë të brendshëm LAN për të siguruar:
  - Endpoints - Hosts zakonisht përbëhen nga laptopë, desktopë, printera, servera dhe telefona IP.
  - Infrastruktura e rrjetit - Pajisjet e infrastrukturës LAN ndërlidhin pikat përfundimtare dhe zakonisht përfshijnë çelsin, pajisjet celulare dhe pajisjet e telefonisë IP.



Antimalware Protection

Host-Based Malware Protection

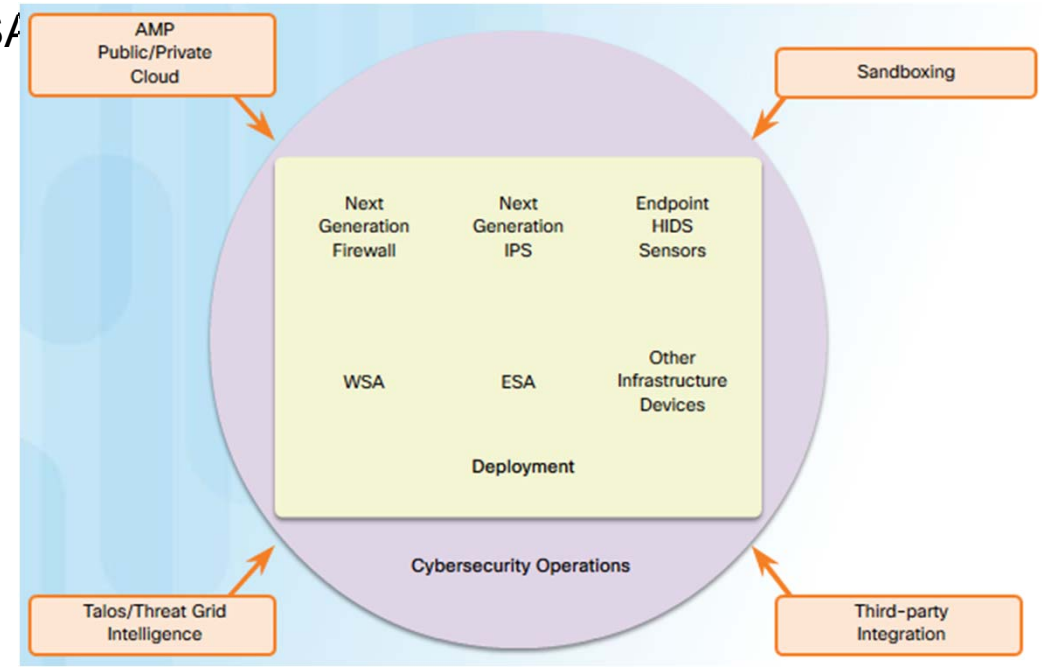
- Antimalware / antivirus software.
  - Nënshkrim i bazuar - Njohja e karakteristikave të ndryshme të skedarëve të njohur malware.
  - Bazuar në heuristics - Njoh karakteristika të përgjithshme të përbashkëta nga llojet e ndryshme të malware.
  - Bazuar në Sjellje - Përdor analiza të sjelljeve të dyshimta.
- Firewall me bazë Host - kufizon lidhjet hyrëse dhe dalëse.
- Suitat me bazë në strehë - përfshijnë antivirus, anti-phishing, shfletim të sigurtë, sistem të parandalimit të ndërhyrjeve në bazë Host, aftësi firewall dhe funksionalitet të fuqishëm të prerjeve.



Antimalware Protection

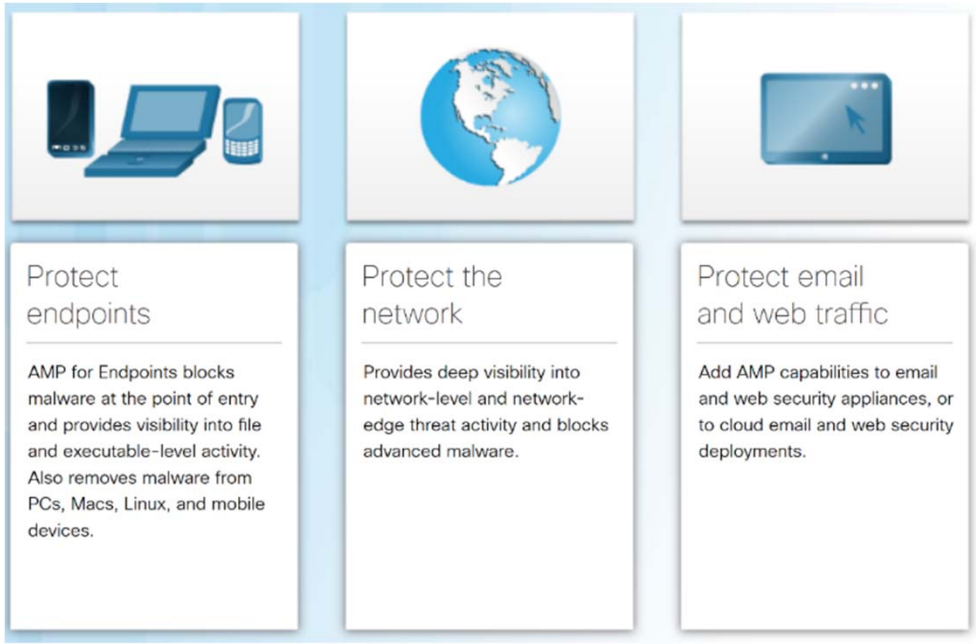
Mbrojtje nga malware të bazuara në rrjet

- Mbrojtje nga malware të bazuara në rrjet
  - Mbrojtja e avancuar e Malware (AMP)
  - Appliance e Sigurisë së Email (ESA
  - Aplikacioni i Web Security (WSA)
  - Kontrolli i pranimit të rrjetit (NAC)



Antimalware Protection

Cisco Advanced Malware Protection (AMP)



- Cisco Advanced Malware Protection (AMP) adreson të gjitha fazat e një sulmi malware:
  - **Para një sulmi** - AMP përdor inteligjencën globale të kërcënimit nga Talos Intelligence and Research Group i Cisco dhe kërcënimi i kërcënimit të Threat Grid.
  - **Gjatë një sulmi** - AMP përdor atë inteligjencë së bashku me nënshkrimet e njohura të skedarëve dhe teknologjinë dinamike të analizës malware të Cisco Threat Grid.
  - **Pas një sulmi** - Zgjidhja shkon përtej aftësive zbuluese në kohë dhe vazhdimisht monitoron dhe analizon të gjithë aktivitetin e skedarit dhe trafikun.

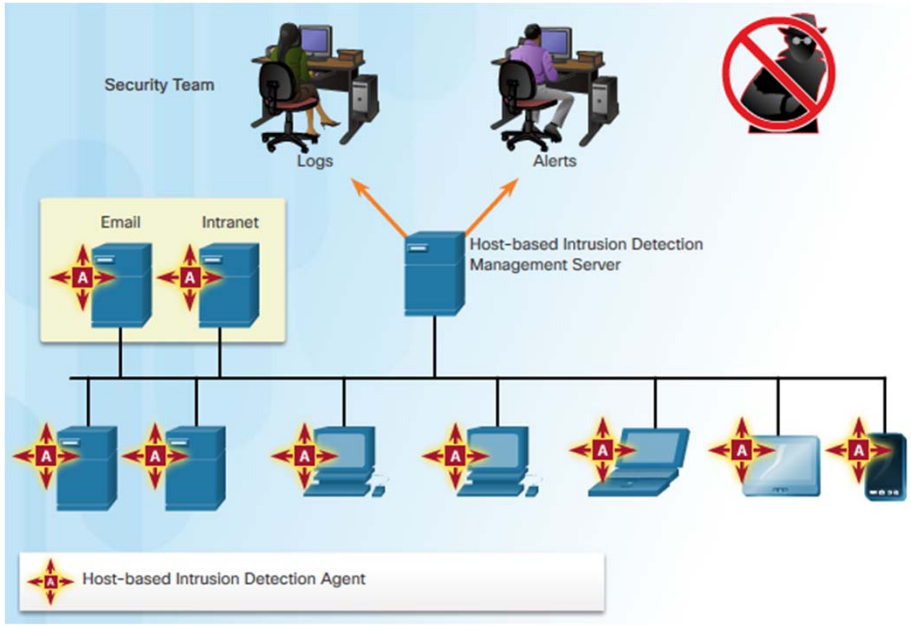
Mbrojtja nga nërhyrjet e bazuara në Host

Host-Based Firewalls

- Firewalls personale me bazë host janë programe të pavarura softuerike që kontrollojnë trafikun që futet ose largohet nga kompjuteri.
- Firewalls me bazë host përfshijnë;
  - Windows Firewall - përdor një qasje të bazuar në profilin për konfigurimin e funksionalitetit të firewall.
  - Iptables - lejon administratorët e sistemit Linux të konfigurojnë rregullat e qasjes në rrjet.
  - Nftables - pasues i iptables, nftables është një aplikim firewall Linux që përdor një makinë të thjeshtë virtuale në kernel Linux.
  - TCP Wrapper për pajisjet me bazë Linux-bazë - kontrollin e qasjes së bazuar në rregulla dhe sistemin e prerjes.

Mbrojtja nga nërhyrjet e bazuara në Host

Host-Based Intrusion Detection



- Sistemi i zbulimit të ndërhyrjeve të bazuara në host (HIDS) mbron hostët kundër malware dhe mund të kryejë sa më poshtë:
  - monitorimin dhe raportimin
  - analiza log
  - korrelacioni i ngjarjes
  - kontrollin e integritetit
  - zbatimin e politikave
  - zbulimin e rootkit
- Softueri HIDS duhet të kandidojë drejtpërdrejt në host, kështu që konsiderohet si një sistem i bazuar në agjentë.

Mbrojtja nga nërhyrjet e bazuara në Host

HIDS Operation

- Një HIDS mund të parandalojë ndërhyrjen sepse përdor nënshkrime për të zbuluar malware të njohur dhe për të parandaluar infektimin e një sistemi.
- Një sërë strategjish shtesë përdoren për të zbuluar malware që shmang zbulimin e nënshkrimit:
  - Sjellja e bazuar në anomali - sjellja është krahasuar me një model bazë të mësimit.
  - Sjellja e bazuar në politika - sjellja normale përshkruhet nga rregullat ose nga shkelja e rregullave të paracaktuara.

Mbrojtja nga nërhyrjet e bazuara në Host

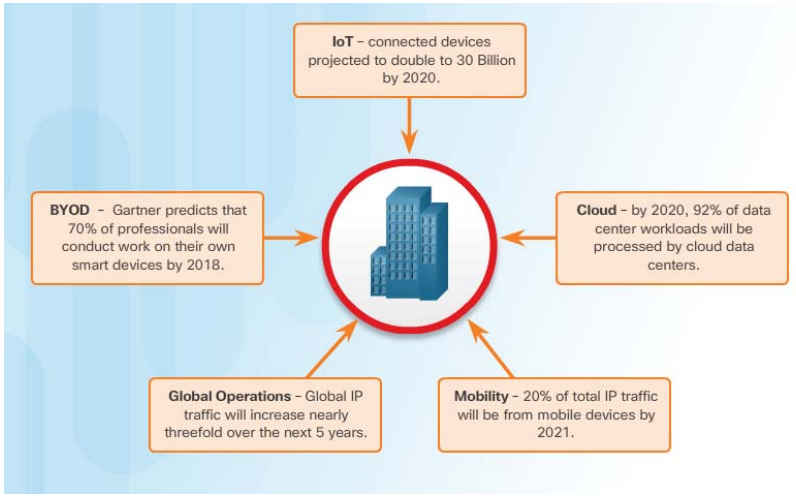
Produktet HIDS

- Shumica e HIDS përdorin softuerin në host dhe disa lloj funksionaliteti të centralizuar të menaxhimit të sigurisë që lejon integrimin me shërbimet e monitorimit të sigurisë së rrjetit dhe inteligjencën e kërcënimeve.
  - Shembuj: Cisco AMP, AlienVault USM, Tripwire dhe Open Source HIDS SECurity (OSSEC).
  - OSSEC përdor një server qendror menaxher dhe agjentë që janë të instaluar në hostë individualë.

Siguria e aplikacioneve

Sipërfaqja e sulmit

- Sipërfaqja e sulmit është shuma totale e dobësive.
  - Përfshirja e porteve të hapura, aplikacioneve, lidhjeve pa tela dhe përdoruesve.
- Zgjerimi për shkak të sistemeve të bazuara në cloud, pajisjeve mobile, BYOD dhe IOT.
- Instituti SANS përshkruan tre komponentë të sipërfaqes së sulmit:
  - Sipërfaqja e sulmit në rrjet
  - Sipërfaqja e sulmit të softuerit
  - Sipërfaqja e sulmit njerëzor



Siguria e Aplikacionit

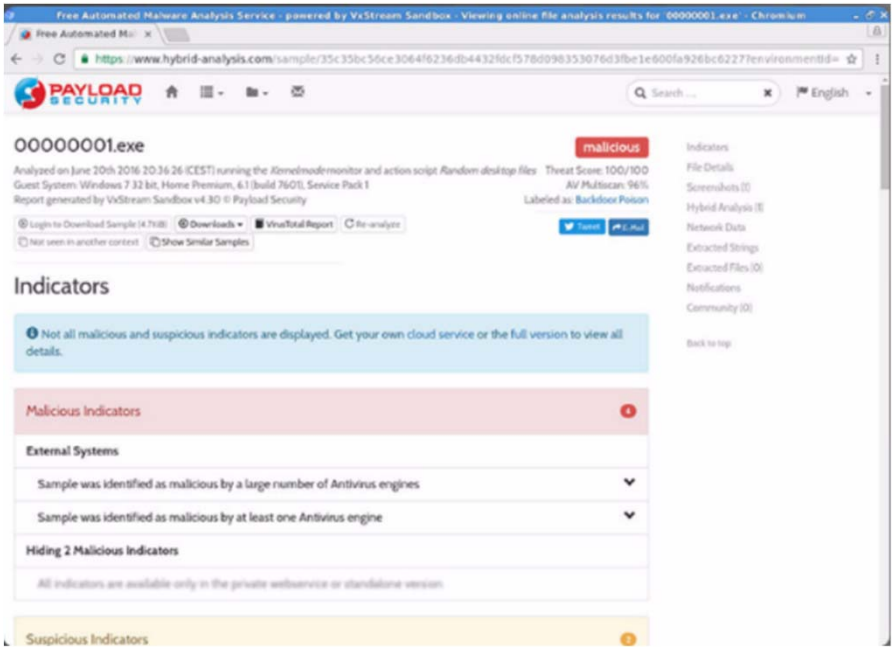
Aplikimi I listës e zezë dhe listës e bardhë

- Lista e zezë e aplikacioneve - cilat aplikacione nuk lejohen.
- Aplikimi i bllokuar i të dhënave - cilat aplikacione lejohen të funksionojnë.
- Të gjithë listat janë krijuar në përputhje me një bazë sigurie që është themeluar nga një organizatë.
- Faqet e internetit gjithashtu mund të jenë në listën e bardhë dhe në listën e zezë.
  - Sistemi i menaxhimit të sigurisë Cisco FireSIGHT është një shembull i një pajisjeje që mund të hyjë në shërbimin e inteligjencës së sigurisë Cisco Talos për të marrë listat e zeza.

Siguria e Aplikacionit

System-Based Sandboxing

- Sandboxing është një teknikë që lejon analizimin e dosjeve të dyshimta dhe të kandidojë në një mjedis të sigurt.
- Për shembull, Cuckoo Sandbox është një sistem i lirë i analizës malware sandbox. Ajo mund të drejtohet në nivel lokal dhe të ketë mostrat e malware të paraqitura për analizë.



Siguria e Aplikimit
Demonstrimi i videove - Përdorimi i një Sandbox për të hapur Malware